VLANs (Virtual LANs)

Cabrillo College

CIS 83

Fall 2006

CCNA 3

Rick Graziani

Cabrillo College

Note to instructors

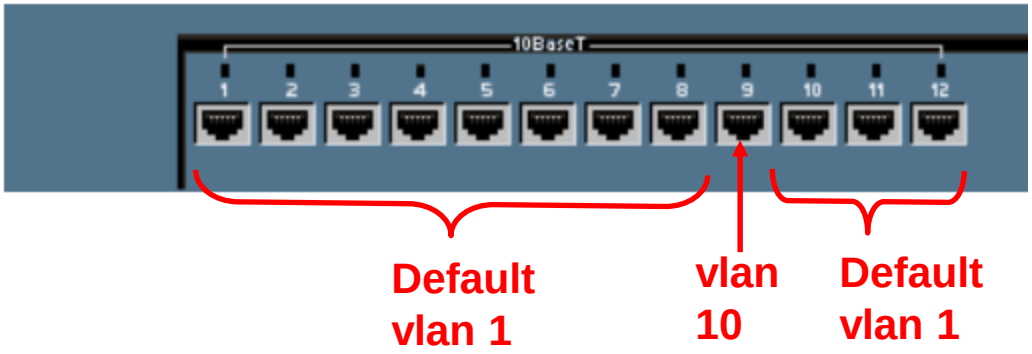
- If you have downloaded this presentation from the Cisco Networking Academy Community FTP Center, this may not be my latest version of this PowerPoint.
- For the latest PowerPoints for all my CCNA, CCNP, and Wireless classes, please go to my web site:

  http://www.cabrillo.edu/~rgraziani/

  - The username is *cisco* and the password is *perlman* for all of my materials.
- If you have any questions on any of my materials or the curriculum, please feel free to email me at graziani@cabrillo.edu (I really don't mind helping.) Also, if you run across any typos or errors in my presentations, please let me know.
- I will add "(Updated – *date*)" next to each presentation on my web site that has been updated since these have been uploaded to the FTP center.

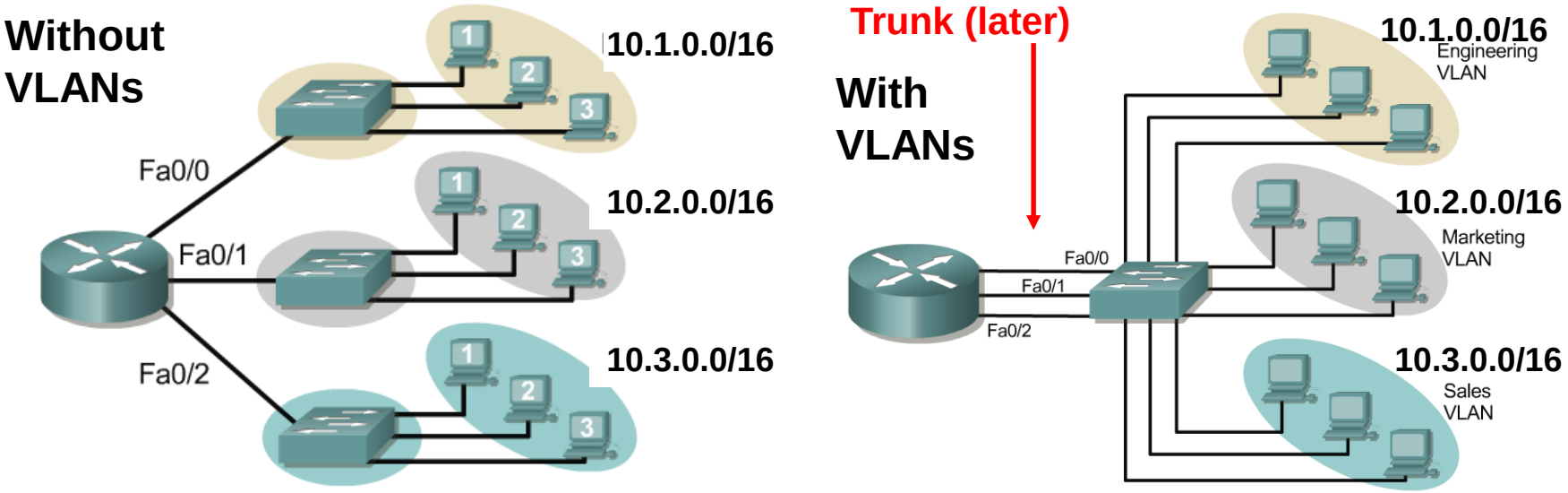
Thanks! Rick

VLAN introduction



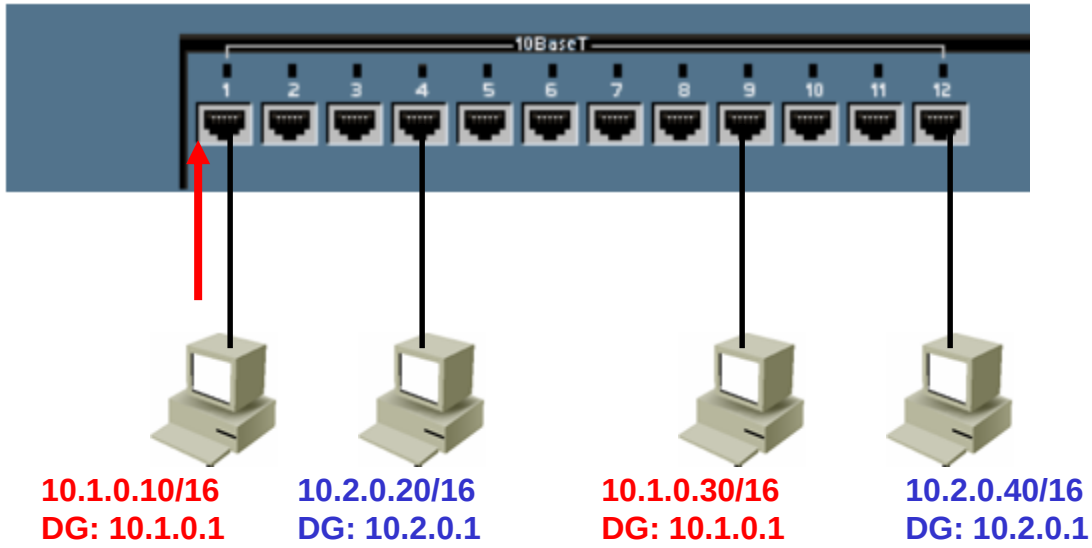
- **VLANs provide segmentation based on broadcast domains.**
- VLAN = Subnet
- VLANs can logically segment switched networks based on:
  - Physical location (Example: Building)
  - Organization (Example: Marketing)
  - Function (Example: Staff)

VLAN introduction



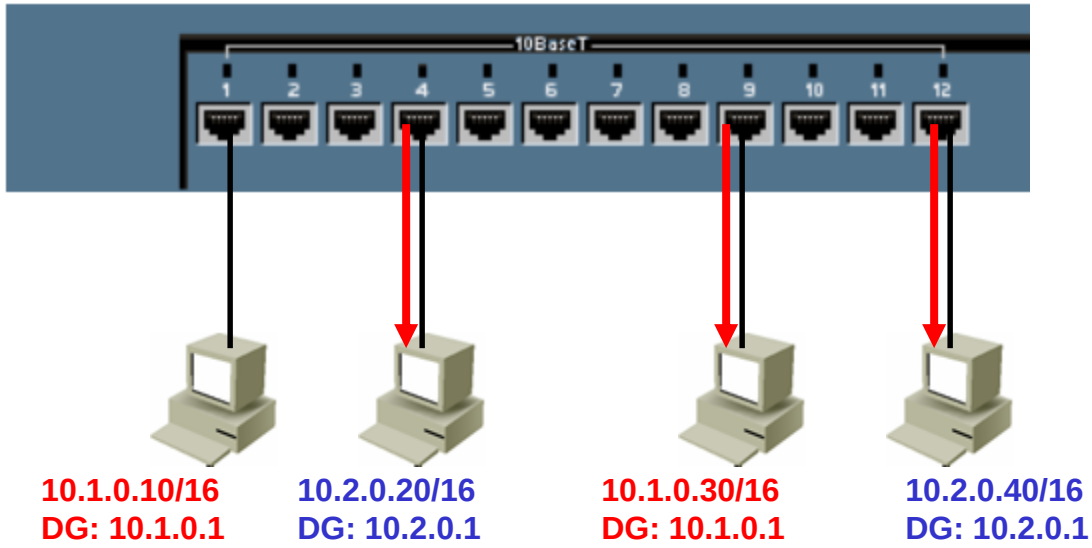
- VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.
- VLANs address scalability, security, and network management.

Two Subnets, One Switch, No VLANs



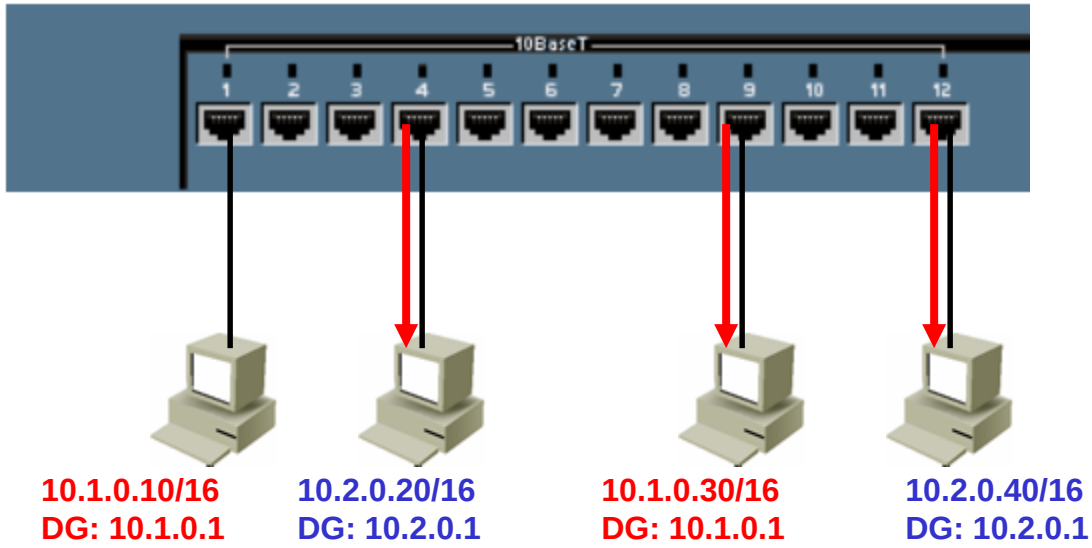
- Layer 2 Broadcasts
  - What happens when 10.1.0.10 sends an ARP Request for 10.1.0.30?

Two Subnets, One Switch, No VLANs



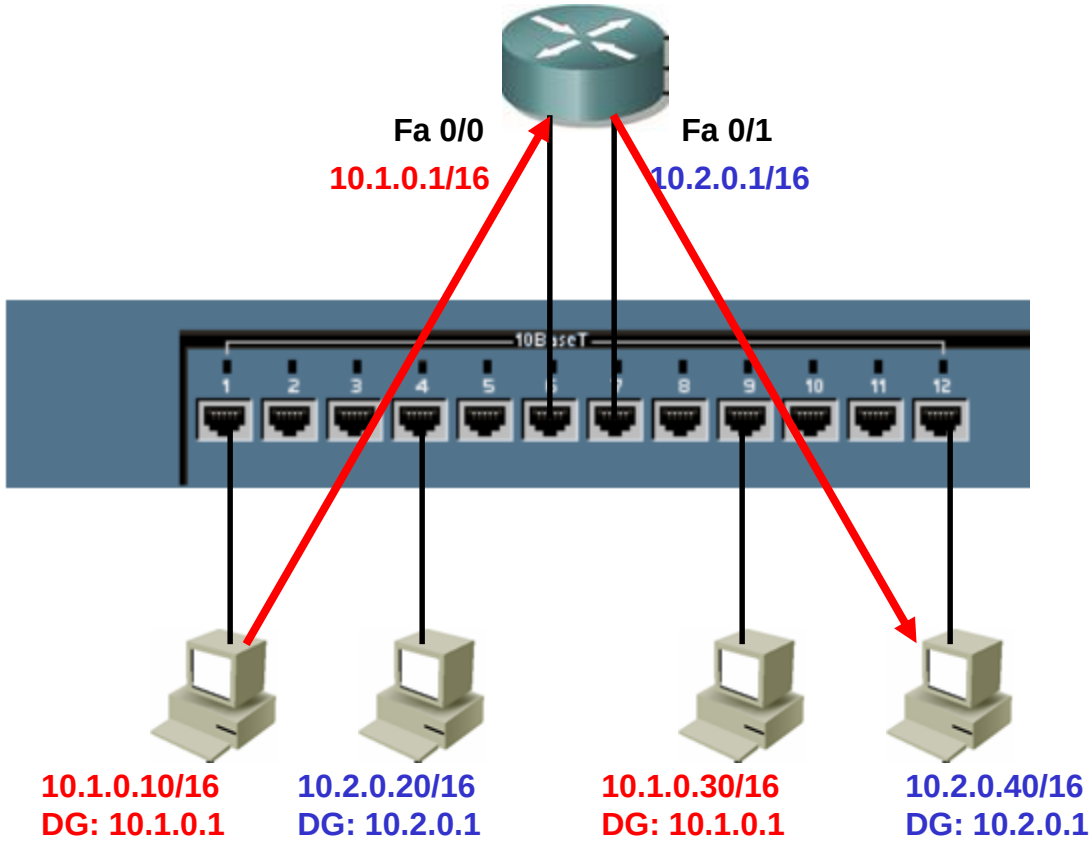
- Layer 2 Broadcasts
  - Switch floods it out all ports.
  - All hosts receive broadcast, even those on a different subnet.
  - Layer 2 broadcast should be isolated to only that network.
  - Note: If the switch supports VLANs, by default all ports belong to the same VLAN and it floods it out all ports that belong to the same VLAN as the incoming port (coming).

Two Subnets, One Switch, No VLANs



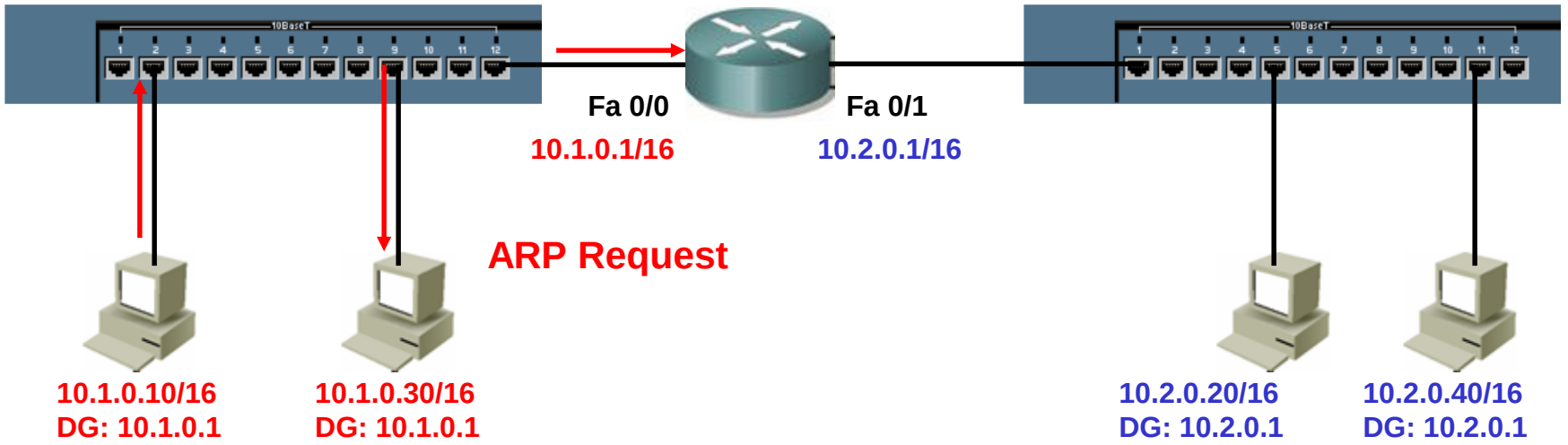
- Layer 2 Unknown Unicasts
  - This is the same for unknown unicasts.

Two Subnets, One Switch, No VLANs



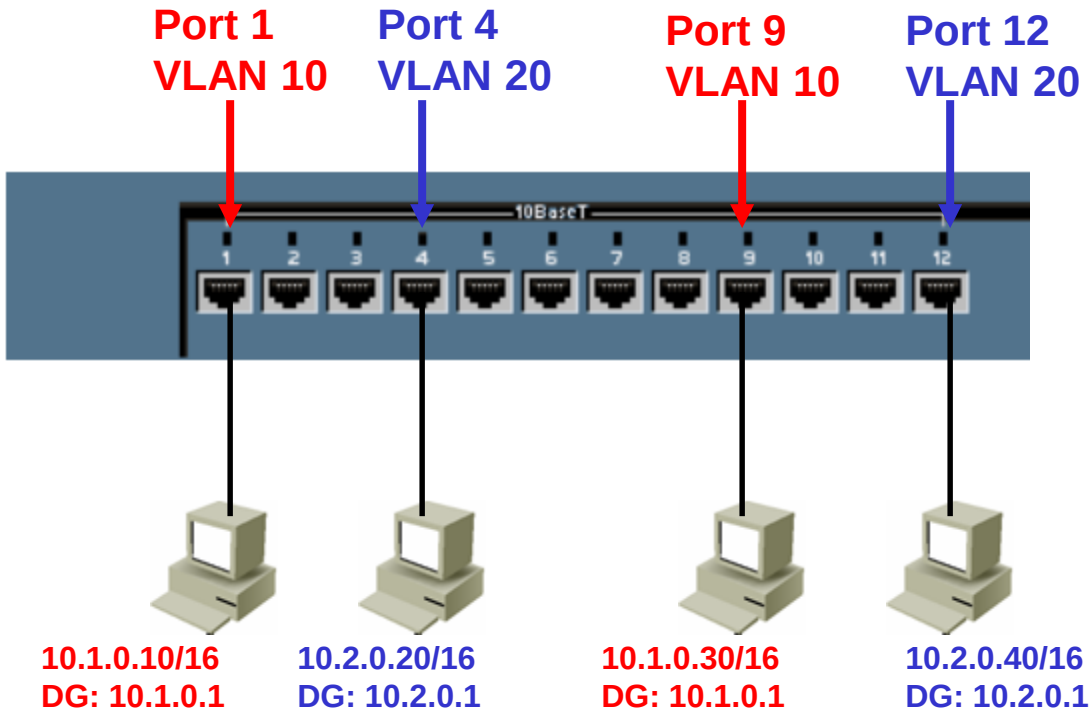
- Even though hosts are connected to the same switch (or even hub), devices on different subnets must communicate via a router.
- Remember a switch is a layer 2 device, it forwards by examining Destination MAC addresses, not IP addresses.

Traditional Solution: Multiple Switches



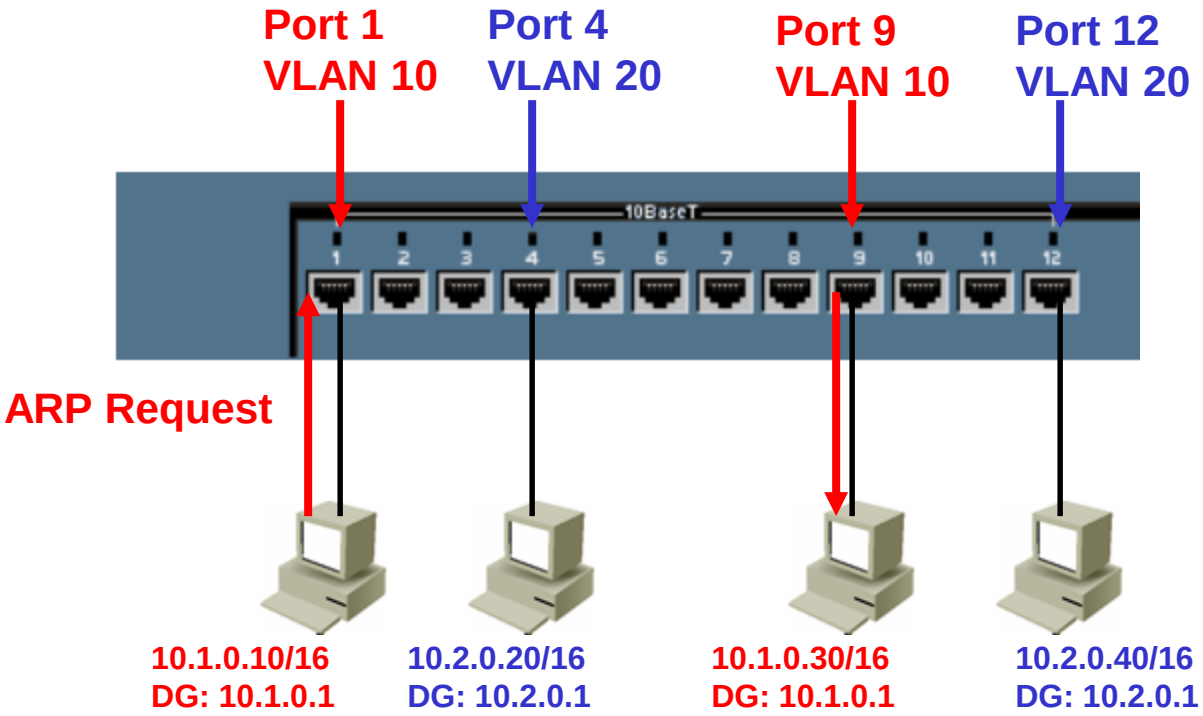
- The traditional solution is have devices on the same subnet connected to the same switch.
- This provides broadcast and unknown unicast segmentation, but is also less scalable.

Broadcast domains with VLANs and routers



- A **VLAN** is a **broadcast domain** created by one or more switches.
- VLANs are assigned on the switch and correspond with the host IP address.
- Each switch port can be assigned to a different VLAN.

Broadcast domains with VLANs and routers

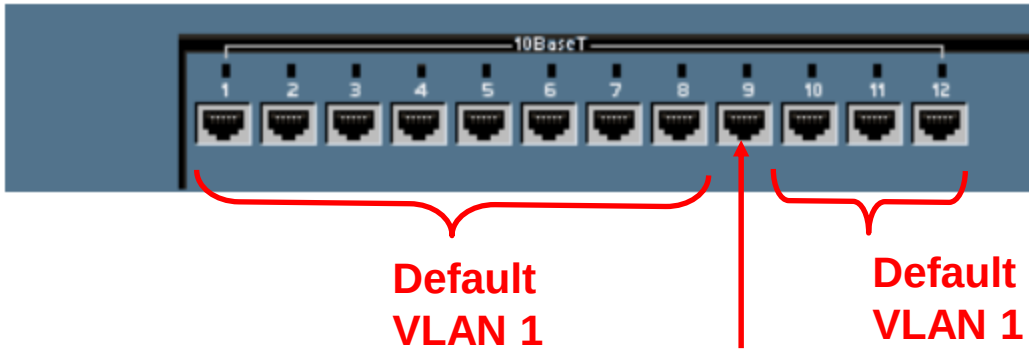


- Ports assigned to the same VLAN share the same broadcast domain.
- Ports in different VLANs do not share the same broadcast domain.

VLAN operation

Configuring VLANs	Description
Statically	Network administrators configure port-by-port. Each Port is associated with a specific VLAN. The network administrator is responsible for keying in the mappings between the ports and VLANs.
Dynamically	The ports are able to dynamically work out their VLAN configuration. Uses a software database of MAC address to VLAN mappings (which the network administrator must set up first).

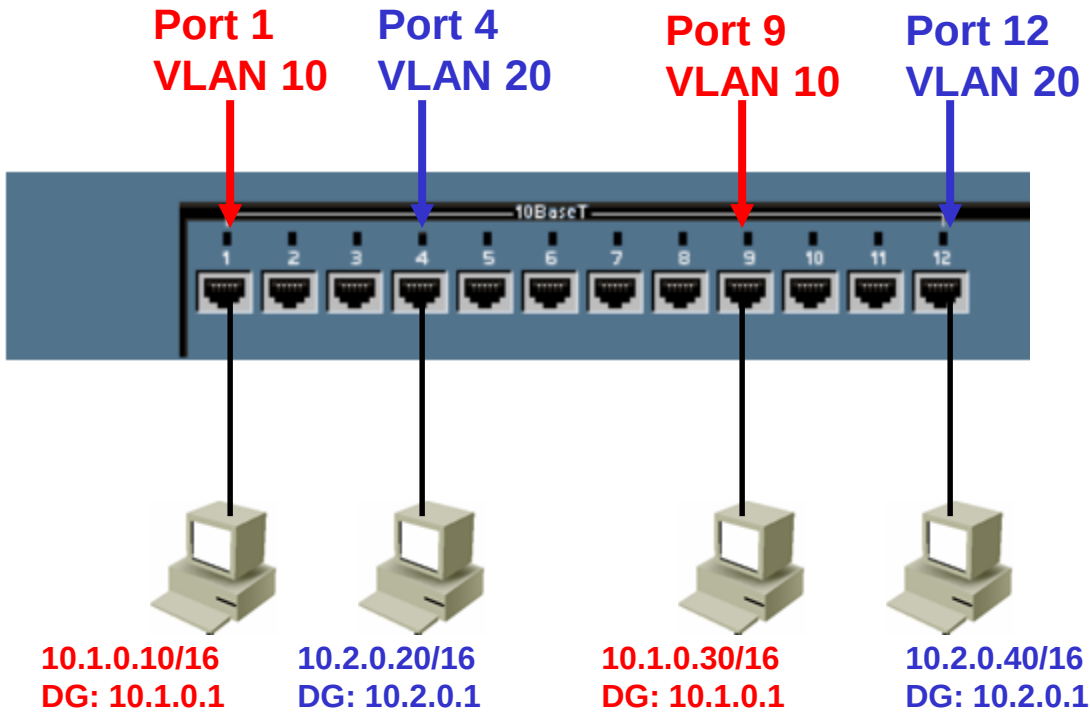
Static VLANS




```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan 10
```

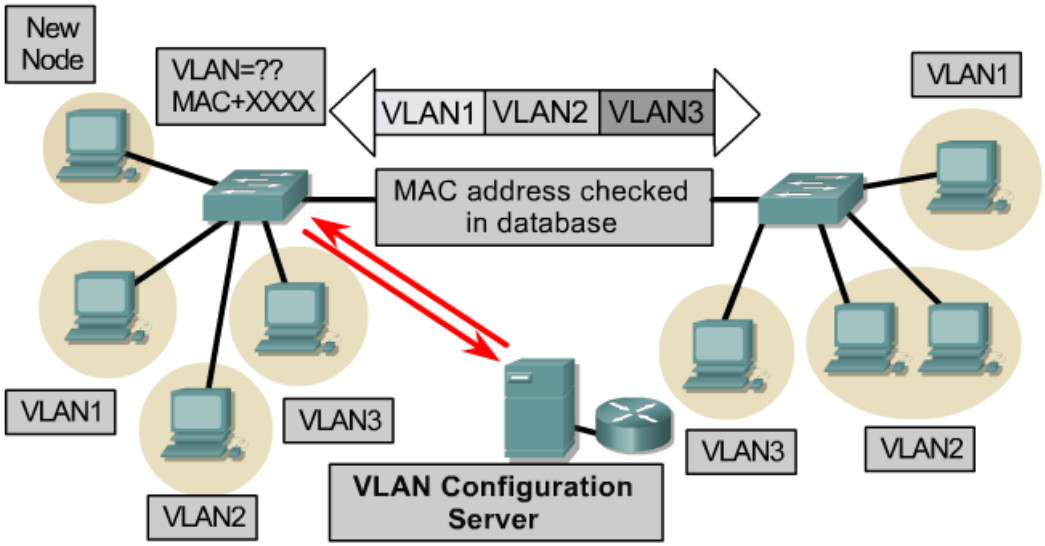
- Static membership VLANs are called **port-based** and **port-centric** membership VLANs.
- This is the most common method of assigning ports to VLANs.
- As a device enters the network, it automatically assumes the VLAN membership of the port to which it is attached.
- There is a **default VLAN**, on Cisco switches that is VLAN 1.

VLAN operation



- VLANs are assigned on the switch port.
- In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.
  - Remember: VLAN = Subnet

VLAN operation



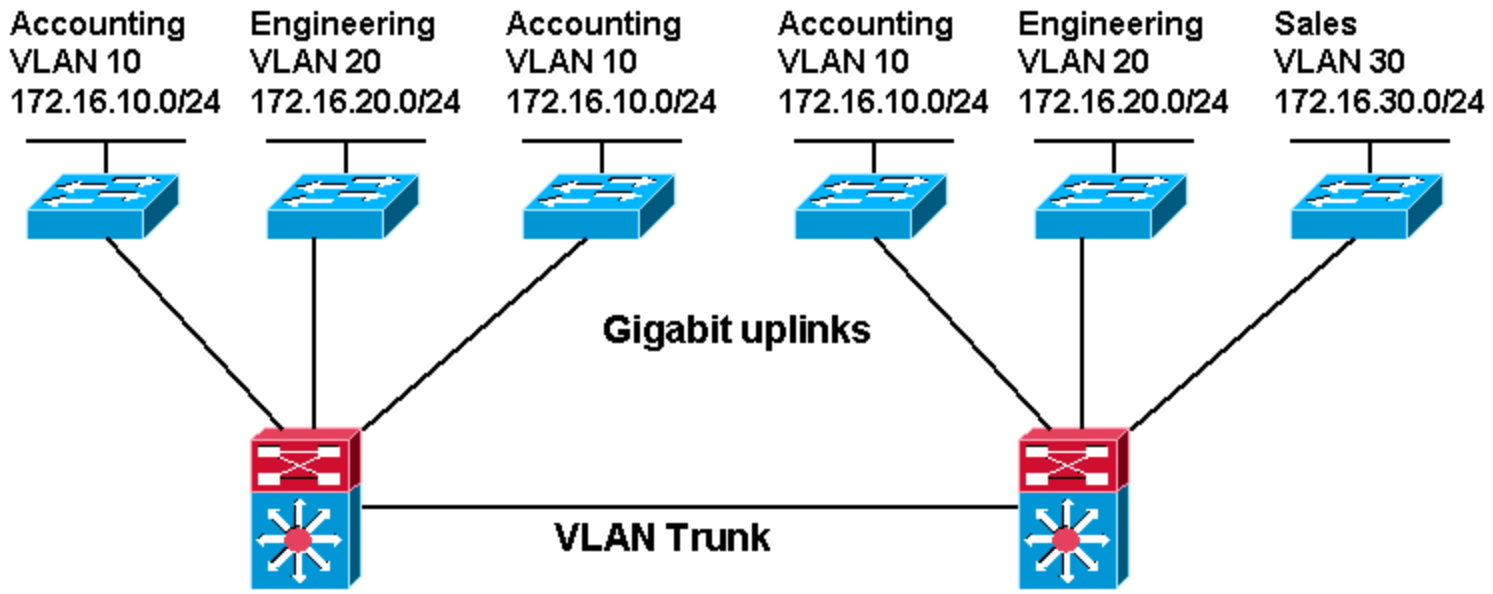
- **Dynamic membership** VLANs are created through network management software. (Not as common as static VLANs)
- CiscoWorks 2000 or CiscoWorks for Switched Internetworks is used to create Dynamic VLANs.
- Dynamic VLANs allow for membership based on the MAC address of the device connected to the switch port.
- As a device enters the network, it queries a database within the switch for a VLAN membership.

Two Types of VLANs

- End-to-End or Campus-wide VLANs
- Geographic or Local VLANs

End-to-End or Campus-wide VLANs

This model is no longer recommended by Cisco and other vendors, unless there is a specific need for this method.

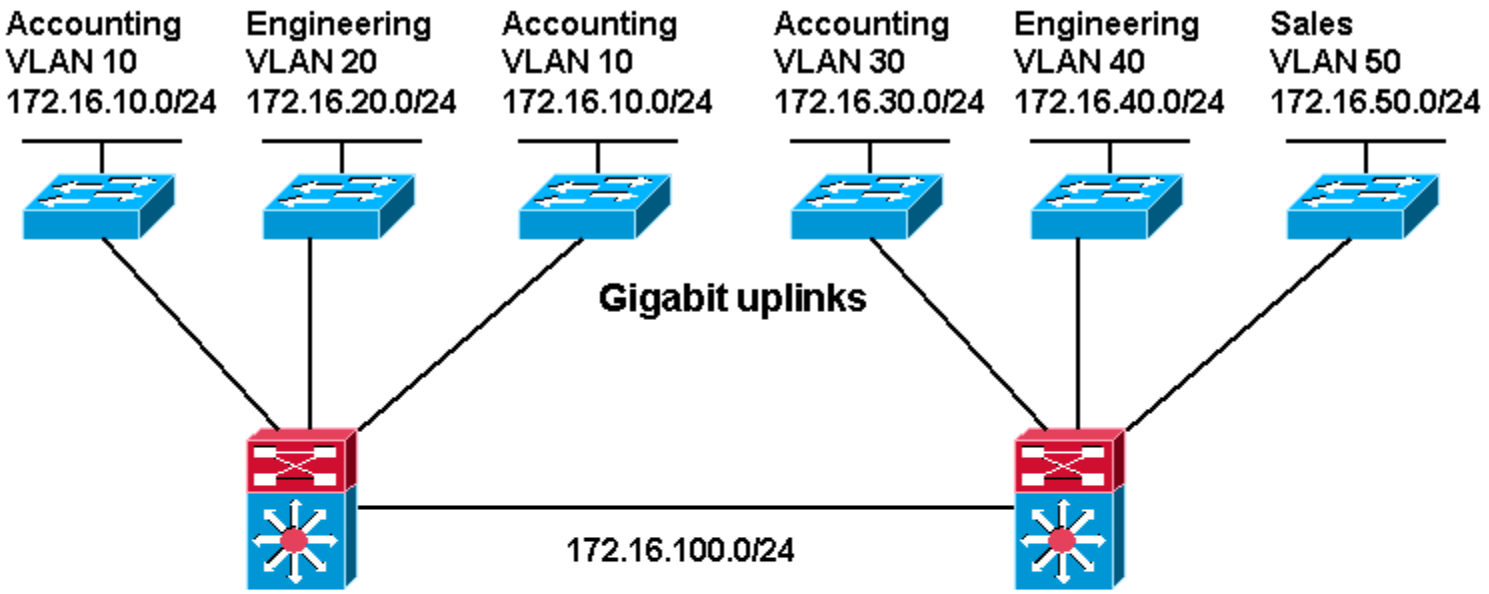


Campus-wide or End-to-End VLAN Model

- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, I.e. Accounting VLAN 10, can be anywhere in the network

Geographic or Local VLANs

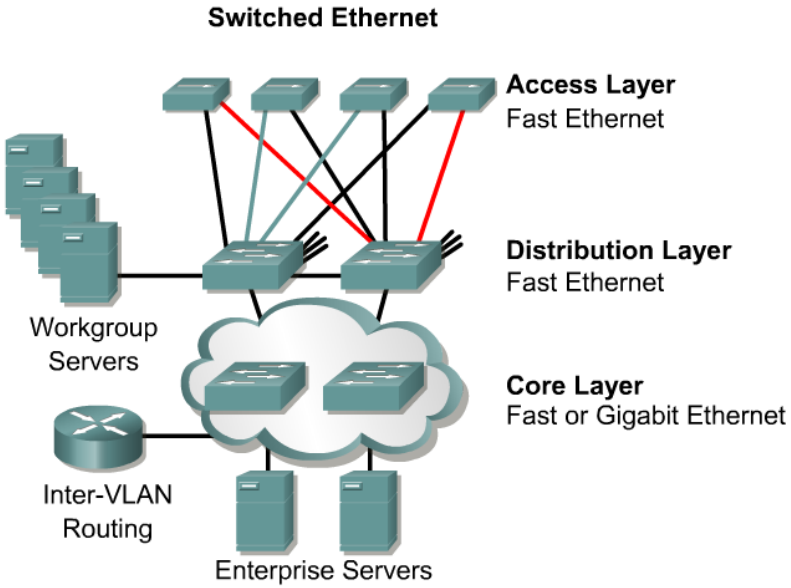
This model is the recommended method. More in CIS 187 (CCNP 3).



Local or Geographic VLAN Model

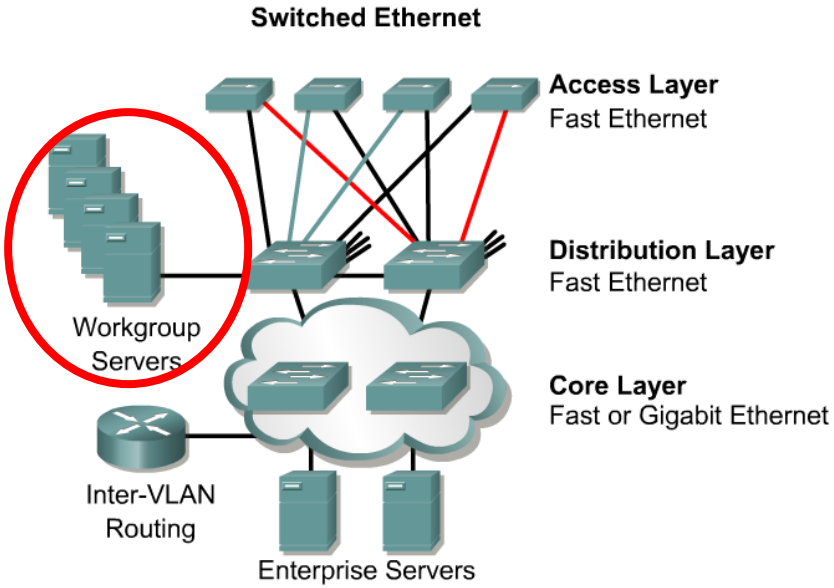
- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, I.e. Accounting VLAN 10 and VLAN 30

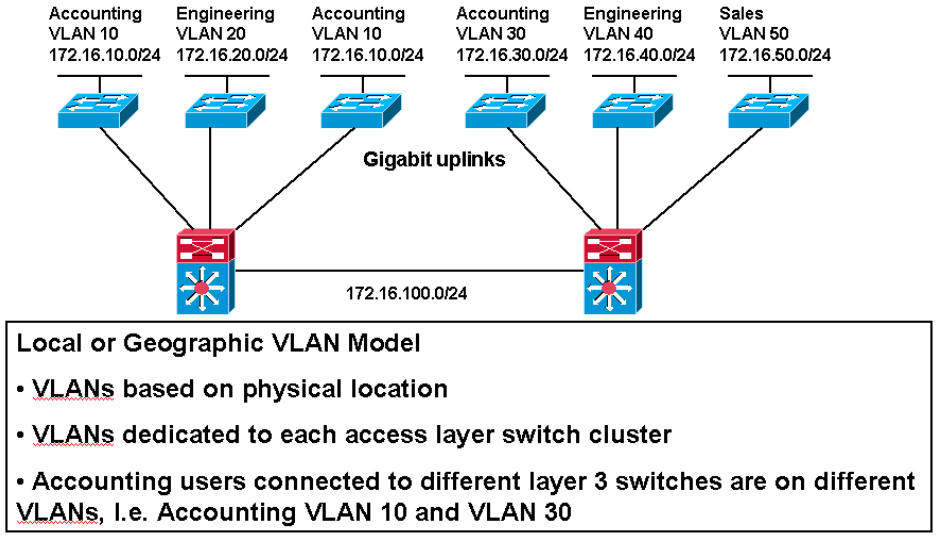
80/20 and 20/80 Rule



- The network is engineered, based on traffic flow patterns, to have **80 percent of the traffic contained within a VLAN.**
- The remaining 20 percent crosses the router to the enterprise servers and to the Internet and WAN.
- This is known as the **80/20 rule.**
- **Note:**
  - With today's traffic patterns, this rule is **becoming obsolete.**
  - **The 20/80 rule** applies to many of today's networks, with 20% of the traffic within a VLAN, and 80% outside the VLAN.

Geographic or Local VLANs

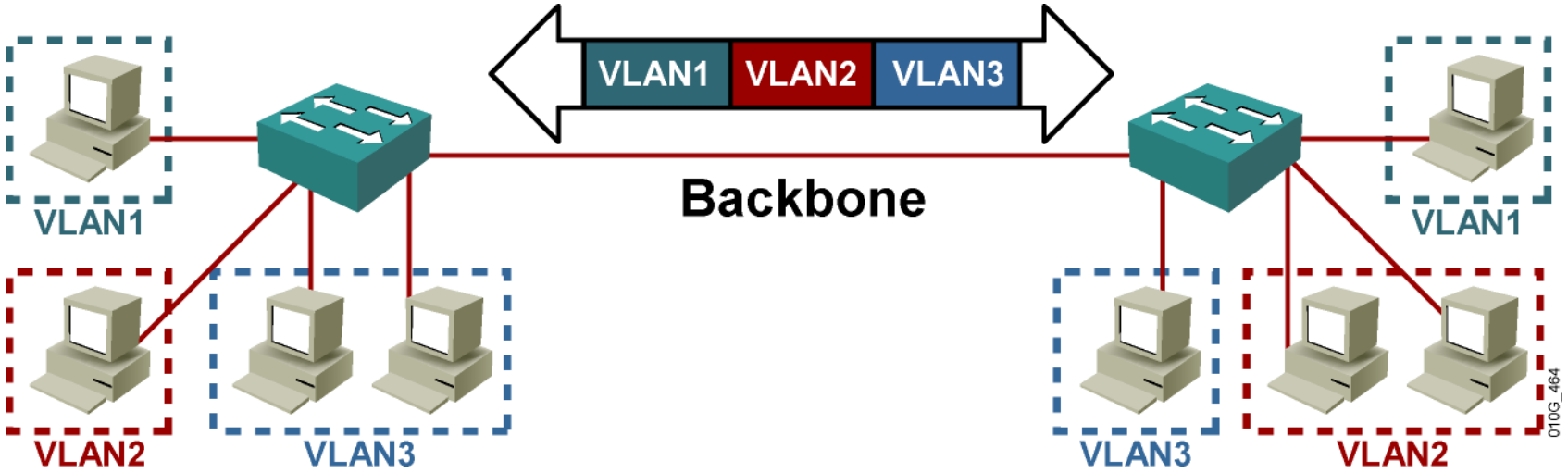




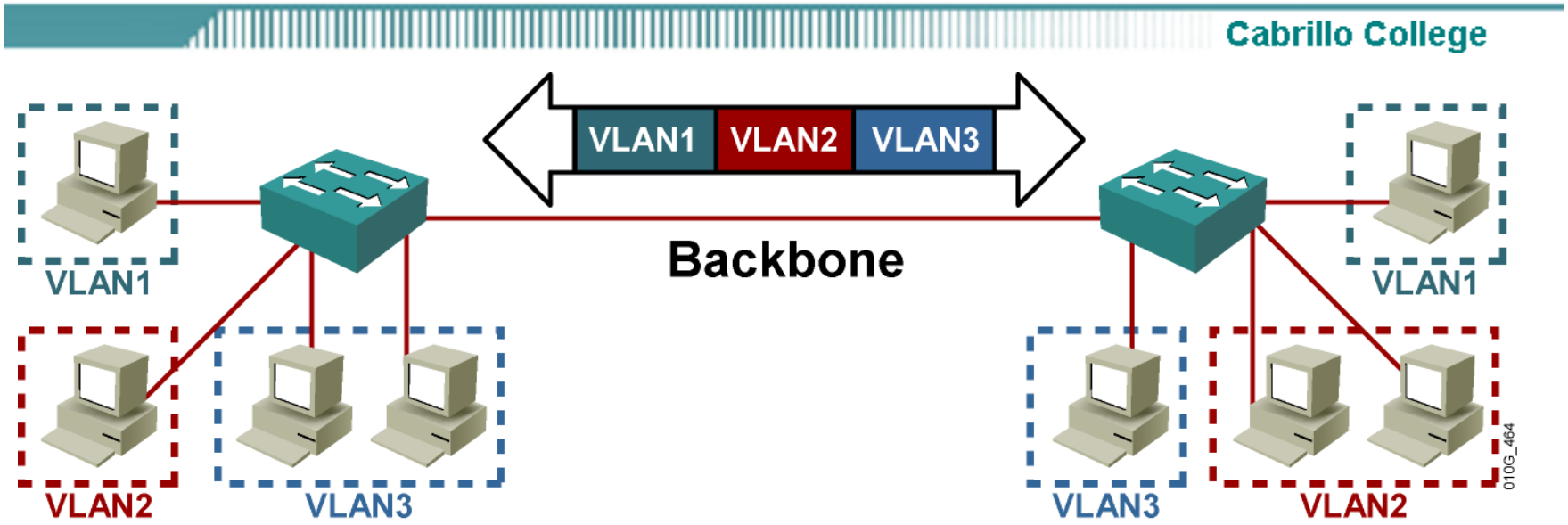
- As many corporate networks have moved to **centralize their resources**, end-to-end VLANs have become more difficult to maintain.
- Users are required to use many different resources, many of which are no longer in their VLAN.
- Because of this shift in placement and usage of resources, VLANs are now more frequently being created around **geographic boundaries** rather than commonality boundaries.

Quick Introduction to Trunking

- More in the next presentation.

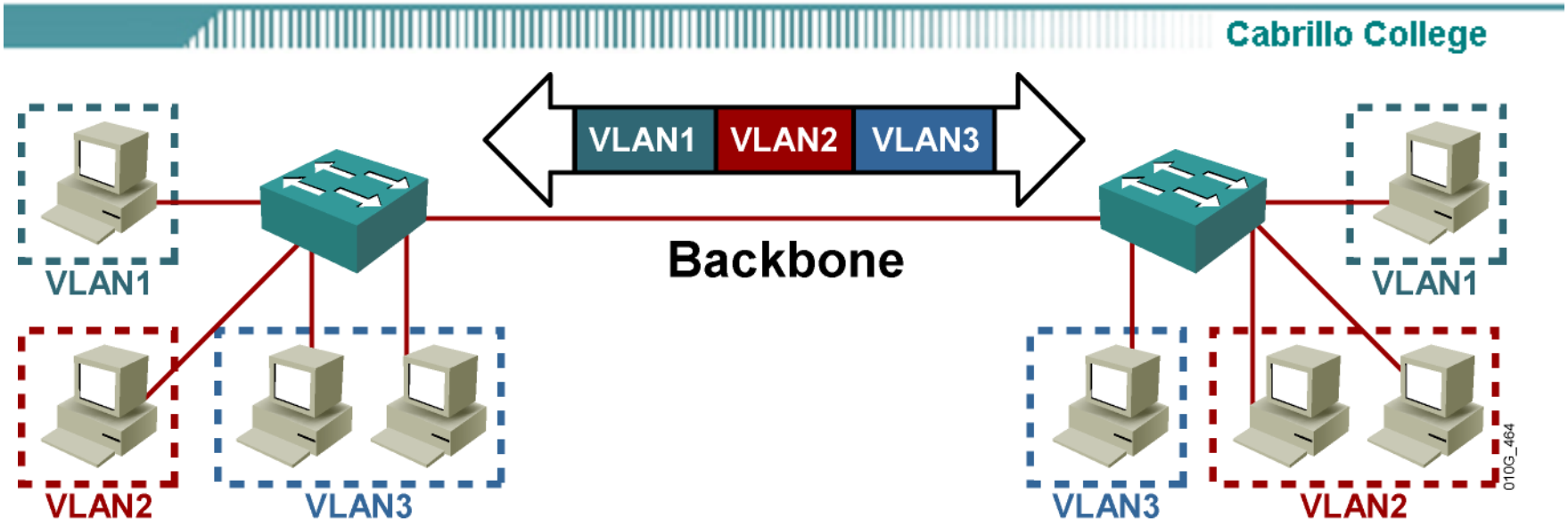


VLAN Trunking/Tagging



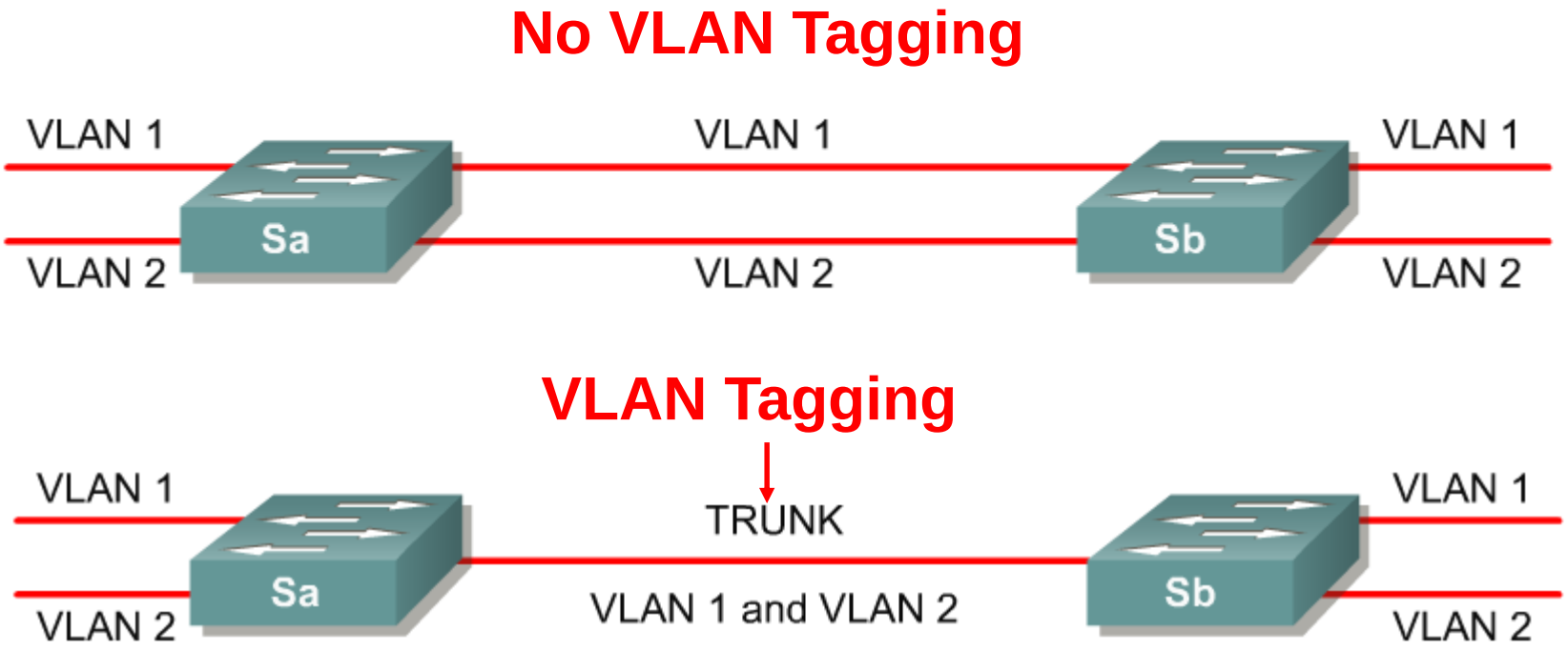
- **VLAN Tagging** is used when a link needs to carry traffic for more than one VLAN.
- **Trunk link:** As packets are received by the switch from any attached end-station device, **a unique packet identifier** is added within each header.
- This header information designates the VLAN membership of each packet.

VLAN Trunking/Tagging



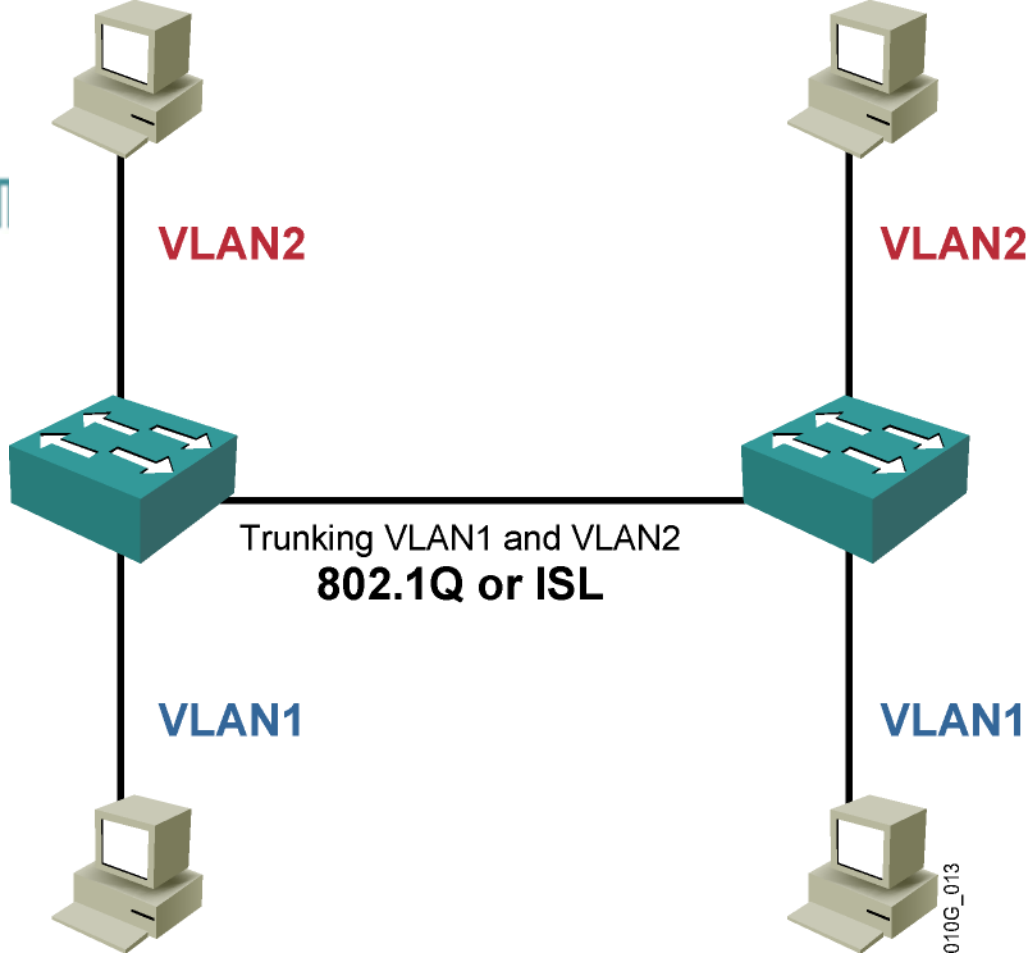
- The packet is then forwarded to the appropriate switches or routers based on the VLAN identifier and MAC address.
- Upon reaching the **destination node (Switch)** the **VLAN ID is removed** from the packet by the adjacent switch and forwarded to the attached device.
- Packet tagging provides a mechanism for controlling the flow of broadcasts and applications while not interfering with the network and applications.
- This is known as a trunk link or VLAN trunking.

VLAN Trunking/Tagging



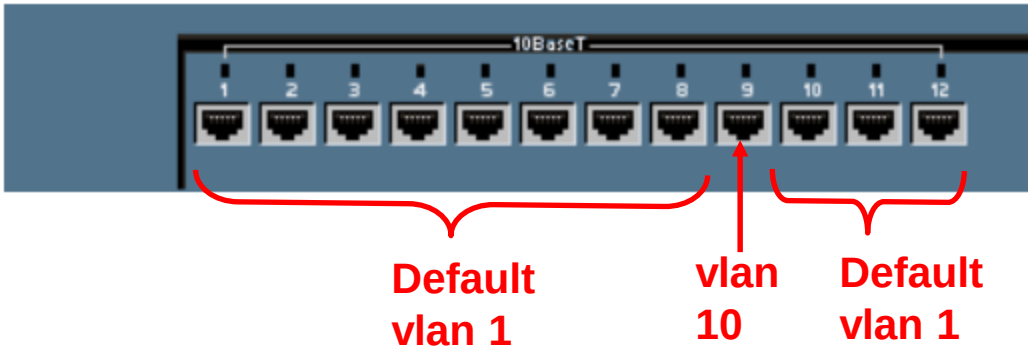
- VLAN Tagging is used when a single link needs to carry traffic for more than one VLAN.

VLAN Trunking/Tagging

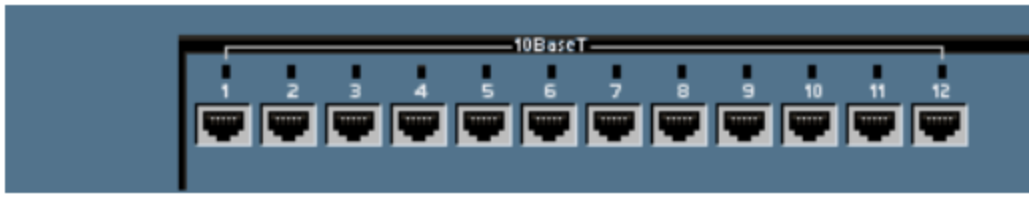


- There are two major methods of frame tagging, Cisco proprietary **Inter-Switch Link (ISL)** and **IEEE 802.1Q**.
- ISL used to be the most common, but is now being replaced by 802.1Q frame tagging.
- Cisco recommends using 802.1Q.
- VLAN Tagging and Trunking will be discussed in the next chapter.

Configuring VLANs

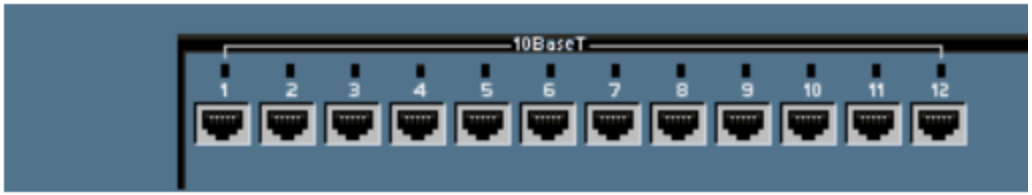


Configuring static VLANs



- The following guidelines must be followed when configuring VLANs on Cisco 29xx switches:
  - The maximum number of VLANs is switch dependent.
    - 29xx switches commonly allow 4,095 VLANs
  - VLAN 1 is one of the factory-default VLANs.
  - VLAN 1 is the default Ethernet VLAN.
  - Cisco Discovery Protocol (CDP) and VLAN Trunking Protocol (VTP) advertisements are sent on VLAN 1. (later)
  - The Catalyst 29xx IP address is in the VLAN 1 broadcast domain by default.

Creating VLANs



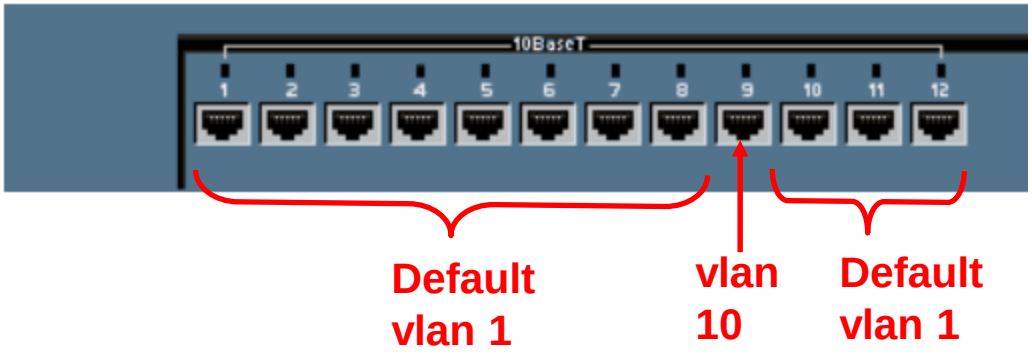
- **Assigning access ports (non-trunk ports) to a specific VLAN**

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan vlan_number
Switch(config-if)#switchport mode access
```

- **Create the VLAN: (This step is <u>not</u> required and will be discussed later.)**

```
Switch#vlan database
Switch(vlan)#vlan vlan_number
Switch(vlan)#exit
```

Creating VLANs

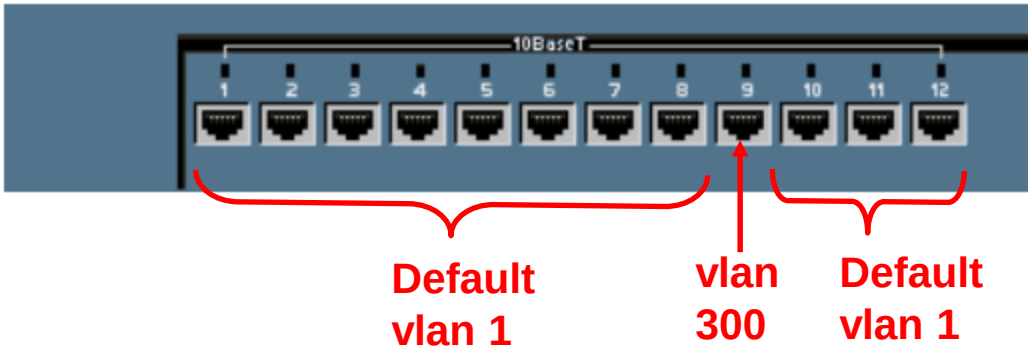


- Assign ports to the VLAN

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport mode access
```

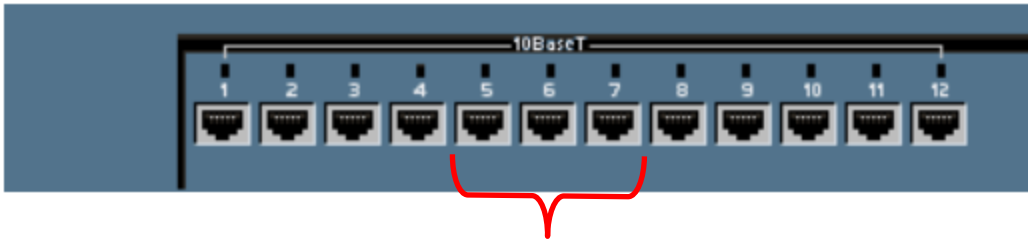
- **access** – Denotes this port as an access port and not a trunk link (later)

Creating VLANs




```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlan 300
Switch(config-if)#switchport mode access
```

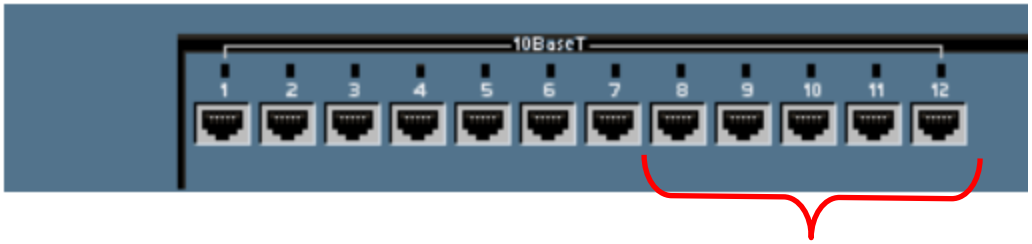
Configuring Ranges of VLANs



vlan 2

```
Switch(config)#interface fastethernet 0/5
Switch(config-if)#switchport access vlan 2
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/6
Switch(config-if)#switchport access vlan 2
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#interface fastethernet 0/7
Switch(config-if)#switchport access vlan 2
Switch(config-if)#switchport mode access
```

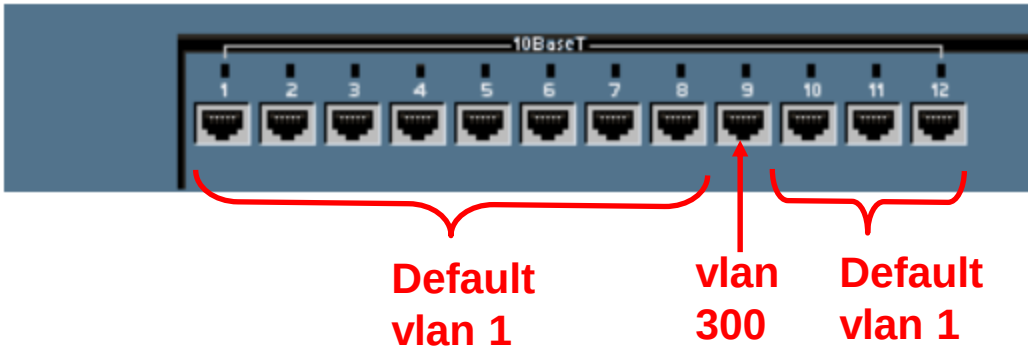
Configuring Ranges of VLANs




```
Switch(config)#interface range fastethernet 0/8 - 12
Switch(config-if)#switchport access vlan 3
Switch(config-if)#switchport mode access
Switch(config-if)#exit
```

- This command does not work on all 2900 switches, such as the 2900 Series XL.
- This format of this command may vary somewhat on various 2900 switches.
- It does work on the 2950.

Creating VLANs

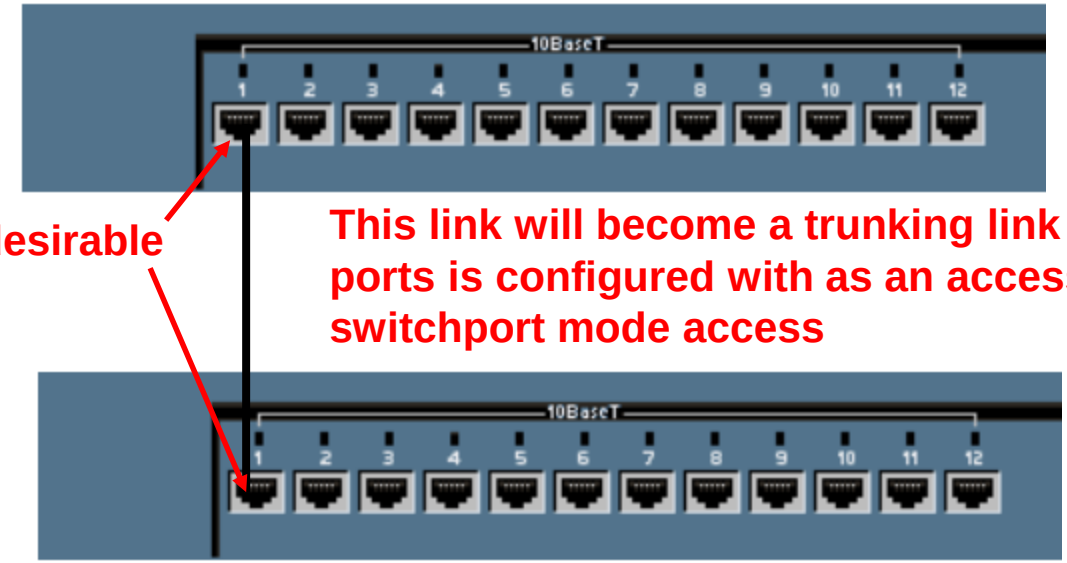



```
SydneySwitch(config)#interface fastethernet 0/1
SydneySwitch(config-if)#switchport mode access
SydneySwitch(config-if)#exit
```

Note: The **`switchport mode access`** command should be configured on all ports that the network administrator does not want to become a trunk port.

- This will be discussed in more in the next chapter, section on DTP.

Creating VLANs

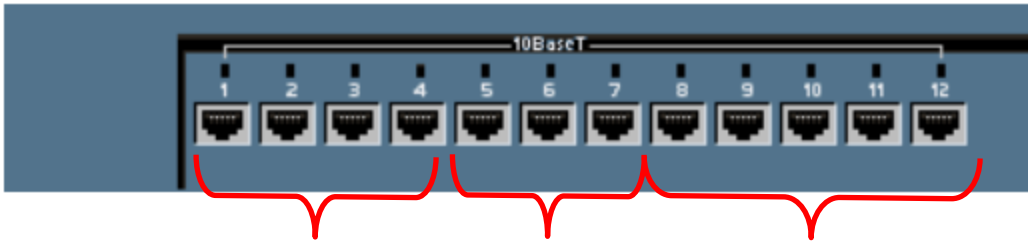


Default: dynamic desirable

This link will become a trunking link unless one of the ports is configured with as an access link, I.e. switchport mode access

- By default, all ports are configured as **`switchport mode dynamic desirable`**, which means that if the port is connected to another switch with an port configured with the same default mode (or desirable or auto), this link will become a trunking link. (See my article on DTP on my web site for more information.)
- Both the **`switchport access vlan`** command and the **`switchport mode access`** command are recommended. (later)
- This will be discussed in more in the next chapter, section on DTP.

Verifying VLANs – show vlan



vlan 1 default **vlan 2** **vlan 3**

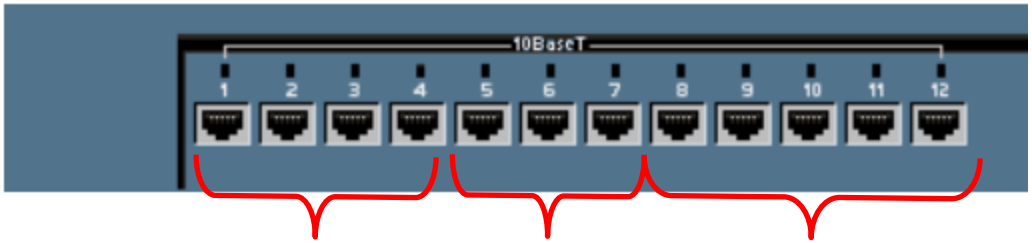
```
SydneySwitch#show vlan

VLAN Name                 Status    Ports
---- -------------------- ------- -------------------------------

VLAN Name                 Status    Ports
---- -------------------- ------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                    Fa0/12
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ---------- ------ -------
1    enet 100001 1500  -      -      -        -   -     1002   1003
2    enet 100002 1500  -      -      -        -   -     0      0
```

Verifying VLANs – show vlan brief




```
SydneySwitch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                            active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Deleting VLANs


```
SydneySwitch#config terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

`Switch(config-if)#` **`no switchport access vlan`** ***`vlan_number`***

- ***This command will reset the interface to VLAN 1.***
- ***VLAN 1 cannot be removed from the switch.***

Accessing/Managing the Switch


```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 10.1.0.5. 255.255.0.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 10.1.0.1
```

The IP Address, Subnet Mask, and Default Gateway on a switch is for the same purposes as when you configure it for a host.

Note: The switch must be configured with a vty login/password and a privileged password for telnet access.

IP Address and Subnet Mask

- By default, VLAN 1 is the “management VLAN”.
- This is where you assign the IP Address and Subnet Mask to the switch.
- This address is for management purposes only and does not affect the Layer 2 switching operations of the switch.
- The address allows you the ability to ping the switch or telnet into the switch.

Default Gateway

- The default gateway is also used for management purposes.
- Once you are telnetted into the switch, if you need to ping or telnet into a device on another network, the default-gateway is where those frames will be sent.

Accessing/Managing the Switch

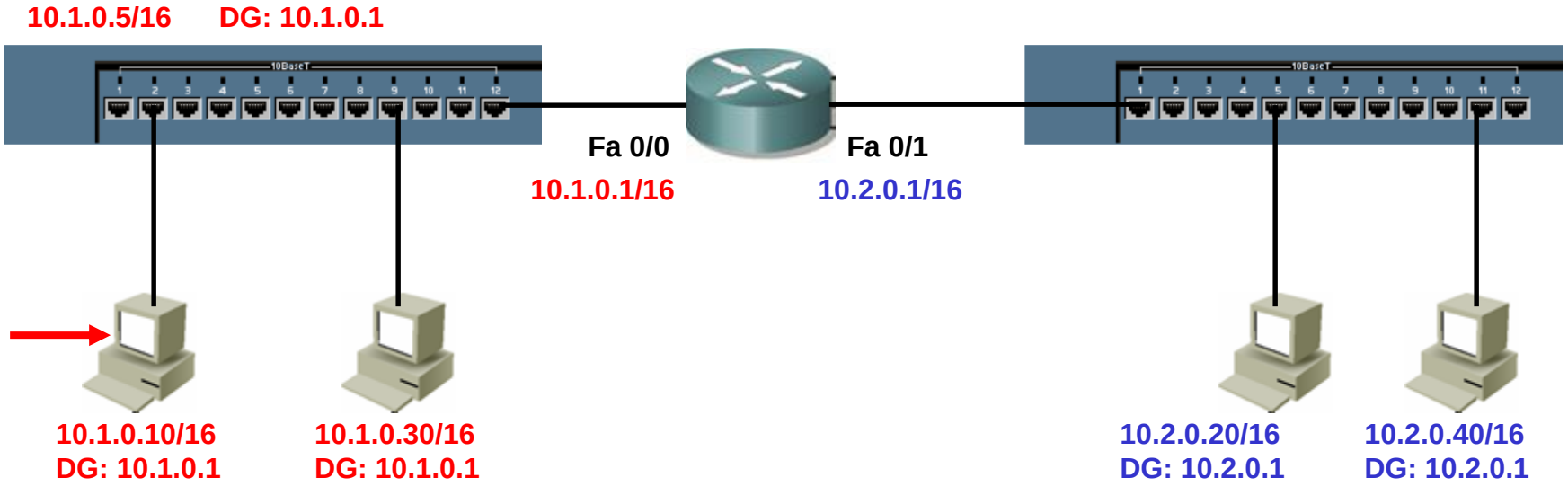

```
Switch(config)# enable secret class

Switch(config)#line vty 0 4
Switch(config-line)#password cisco
Switch(config-line)#login

Switch(config)#inter vlan 1
Switch(config-if)#ip add 10.1.0.5. 255.255.0.0
Switch(config-if)#no shut

Switch(config)#ip default-gateway 10.1.0.1
```

Accessing/Managing the Switch




```
Host
C:\>telnet 10.1.0.1
username:cisco
password:class
Switch>show vlan
Switch>ping 10.2.0.20
Switch>telnet 10.1.0.1
Switch>exit
```

Erasing VLAN information


```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
Switch#reload
```

- VLAN information is kept in the vlan.dat file.
- The file is not erased when erasing the startup-config.
- To remove all VLAN information, use the command above and reload the switch.

VLANs (Virtual LANs)

Cabrillo College

CIS 83

Fall 2006

CCNA 3

Rick Graziani

Cabrillo College